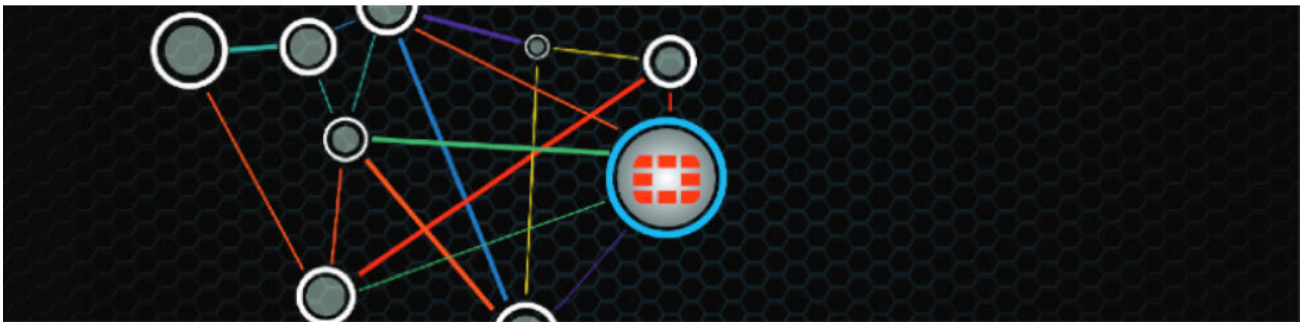
Configuration Guide



FortiGate Session Life Support Protocol (FGSP)

Author: Jason Graun
Network Security Architect

Contents

Introduction

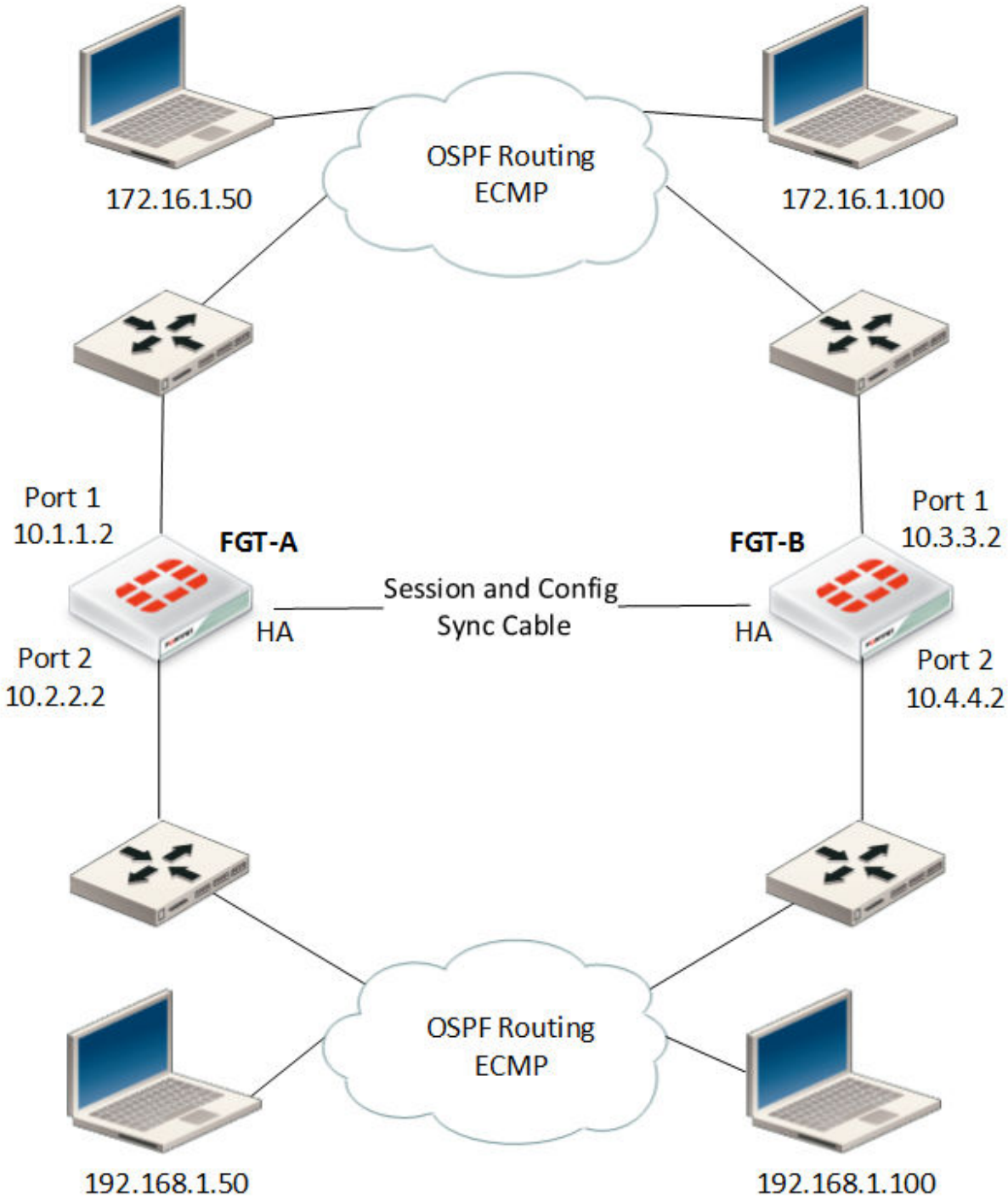
This document assumes knowledge of FortiGate Clustering Protocol (FGCP).

FortiGate Session Life Support Protocol (FGSP) was introduced in FortiOS 5.0. However in previous versions of FortiOS this feature was known as “standalone session sync” and only supported TCP sessions, did not support asymmetric traffic and had other deployment limitations. FGSP was designed to overcome these limitations. It supports asymmetric traffic, TCP, UDP, ICMP sessions as well as NAT sessions. FGSP also supports configuration synchronization between FortiGates. The use of traffic load-balancers to share load across two FortiGates is possible with FGSP. FGSP is well suited for networks using equal cost load balancing of links between routers. Also called equal-cost multi-path (ECMP) routing or multipath routing.

FGSP Deployment scenario

ECMP routing is very common in large networks using OSPF. Typically when ECMP is in use routers will route packets based on a source/destination IP pair. Figure 1 below shows an example network with ECMP. Assume 192.168.1.50 and 192.168.1.100 are both sending traffic to 172.16.1.50 and 172.16.1.100 respectively, it is very likely that the traffic will each take a different path in the network. 172.16.1.50/192.168.1.50 might take the left path in the network and 172.16.1.100/192.168.1.100 would take the right path in the network.

Figure 1


OSPF Routing
ECMP
172.16.1.50
172.16.1.100
Port 1
10.1.1.2
FGT-A
FGT-B
Port 1
10.3.3.2
Session and Config
Sync Cable
HA
HA
Port 2
10.2.2.2
Port 2
10.4.4.2
OSPF Routing
ECMP
192.168.1.50
192.168.1.100

When using FGSP both FortiGates are in an active state and will process packets, which is the desired function when using ECMP routing in a network. FGSP's many advantage in this scenario is that the interfaces do not have to be Layer-2 adjacent to each other as they do in FGCP. Each interface can have its own IP address in a different subnet as shown in Figure 1. This allows the FortiGate to be a stateful firewall and even with traffic taking diverse paths in the network.

In figure 1, a failure of any device along the data path will result in no loss of data because the opposite FortiGate will take over handling all existing traffic. Sessions will have already been synced prior to failure as a result of implementing FGSP.

Deployment considerations

The following are important aspects that should be understood when discussing deployments of FGSP.

- FortiGates running FGSP act as independent devices when compared to FGCP. Interface IP addresses must be unique to each interface, there are no shared IP addresses, and there is no clustering.
- FortiGate configurations are not automatically synchronized. It must first be enabled.
- The same ForitGate models should be used for both peers to avoid uneven performance.
- The names of the interfaces, including VLAN interfaces, aggregate interfaces, etc… must be the same on both peers.
- It is possible to synchronize sessions from only specific VDOMs.
- Session synchronizations filters can be enabled to only synchronize specific traffic.
- You cannot run FGSP and FGCP at the same time on the same FortiGates.
- VRPP is supported in FGSP.
- Performance limitations should be considered in case of a failover scenario. One device must be able to handle the load of both.

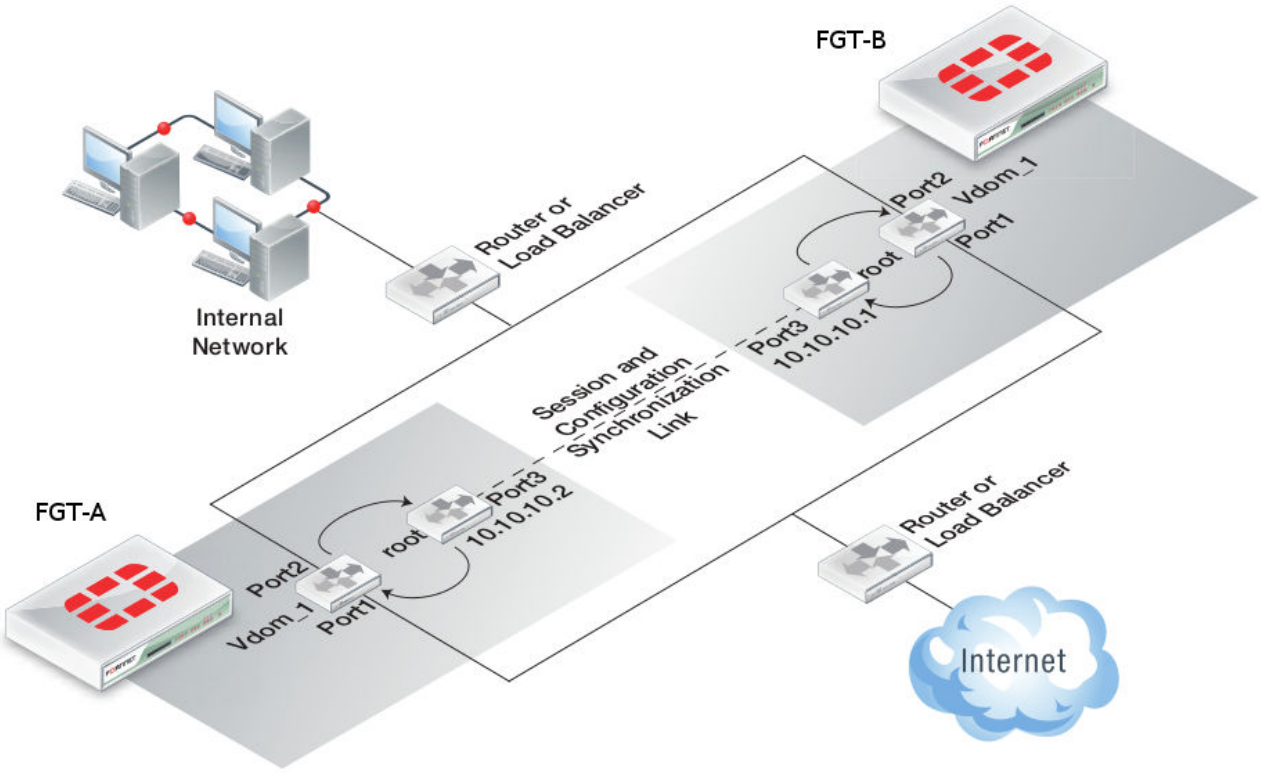
Requirements

A FortiGate running FortiOS 5.0 or later is required. It is recommended to use the latest available GA patch.

This configuration example uses two FortiGate 140D's running FortiOS 5.0 patch 6 (build 0271).

Configuration Procedure

Figure 2



CLI Commands

FGSP parameters are configured from the CLI only. There are some similarities to FGCP configurations.

Step 1 – Begin with Two Factory Default FortiGates

If needed issue the following command to return the FortiGates to factory default.

```
execute factoryreset
```

Answer YES to the prompt and the FortiGates will reboot with a default configuration.

Step 2 – Configure Session Synchronization Peers

FGT-A in figure 2 above has an IP address of 10.10.10.2 configured on port3.
FGT-B in figure 2 above has an IP address of 10.10.10.1 configured on port3.

FGT-A:

```
config system session-sync
    edit 1
        set peerip 10.10.10.1
        set peervd "root"
        set syncvd "vdom_1"
```

FGT-B:

```
config system session-sync
    edit 1
        set peerip 10.10.10.2
        set peervd "root"
        set syncvd "vdom_1"
```

The **syncvd** tells the FortiGate to synchronize sessions that exist in the "vdom_1" VDOM. Sessions in the "root" VDOM will not be synchronized. To synchronize more than one VDOM, add additional statements for each VDOM that requires session synchronization. The **peerip** and **peervd** settings will be the same, only the **syncvd** setting will change.

The **peervd** of **root** tells the FortiGate that sessions will be synchronized using the root VDOM as the transport mechanism. The **peerip** IP address must be in the same VDOM as the **peervd** setting. In figure 2 the port3 is in the "root" VDOM.

When VDOMs are not enabled the **peervd** setting defaults to "root" and is only visible using "show full-configuration".

If VDOMs are not enabled the **peervd** setting defaults to root.

FGT-A:

```
config system session-sync
    edit 1
        set peerip 10.10.10.1
        set syncvd "root"
```

FGT-B:

```
config system session-sync
    edit 1
        set peerip 10.10.10.2
        set syncvd "root
```

Step 3 – Enable Configuration Synchronization

Configuration Synchronization in FGSP synchronizes firewall policies, UTM policies, etc… It does not synchronize, by design, interface IP addresses and BGP peer information as these settings must be unique.

To enable configuration synchronization, on both FortiGates issue the following commands

```
config system ha
    set standalone-config-sync enable
```

Reboot both FortiGates after enabling the command.

Standalone configuration synchronization uses a very similar process as FGCP. There is a master/backup relationship between the two FortiGates similar to FGCP but only of configuration synchronization not session information. In fact you will see a familiar message on the FortiGate's console after the reboot. These are the same messages seen in FGCP configurations.

```
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
```

With configuration synchronization is enabled, configuration changes to one FortiGate will synchronize to the other. Keep in mind both firewalls are active when using FGSP.

Step 4 – Add Session Synchronization

Now the two FortiGates are setup to synchronize configuration and sessions between themselves we must tell the FortiGates what type of sessions should be synchronized. FGSP synchronizes IPv4 and IPv6 TCP, UDP, ICMP, expectation (asymmetric sessions), and NAT sessions. All of the configuration is done in HA system settings. Session-pickup must first be enabled.

Synchronizes NAT sessions.

```
config system ha
    set session-pickup enable
    set session-pickup-nat enable
```

Synchronizes UDP and ICMP sessions.

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
```

Synchronizes exception sessions also called asymmetric sessions

```
config system ha
    set session-pickup enable
    set session-pickup-expectation enable
```

Step 5 – Session Synchronization Filter (optional)

There maybe scenarios when you only want to synchronize sessions of certain types of traffic. For example only sessions for specific IP addresses can by synchronized. In the configuration below only traffic sourced from 192.168.1.50 to 172.16.1.50 would be synchronized.

Specific IP addresses

```
config system session-sync
    edit 1
            config filter
                set dstaddr 172.16.1.50 255.255.255.255
                set srcaddr 192.168.1.50 255.255.255.255
```

At this point the FortiGates have a basic FGSP configuration that will synchronize sessions and configuration between the two firewalls.

Understanding Session Synchronization Details

Session synchronization statistics

Below is the output from **diagnose sys session sync**. Here we can see what types of sessions will be synchronized, how many sessions have been synchronized to the peer FortiGate, how many sessions have been synchronized to this FortiGate and the filter configuration if one is created.

```
FGT-A # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_redir=0, sync_nat=1.
sync: create=12:0, update=0, delete=0:0, query=14
recv: create=14:0, update=0, delete=0:0, query=12
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
nCfg_sess_sync_num=5, mtu=16000
sync_filter:
      1: vd=0, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0,
sport=0-65535, dport=0:65535
```

The **sync_started=1** let's us know that synchronization is working. If this is set to zero then something is not correct with session synchronization. The other sync values show that TCP, connectionless, asymmetric and NAT sessions will all be synchronized.

The two fields **sync: create=12:0** and **recv: create=14:0** show that this FortiGate has synchronized 12 sessions to its peer and has received 14 sessions from its peer.

The **sync_filter** shows the configured filter. In this case no filter is created so all sessions will be synchronized. The `vd=0` indicates that sessions in the root VDOM will be synchronized.

New Session Flag

Below is the output from **diagnose sys session list**. Under "state" we can see a new flag called "synced". The flag indicates that this FortiGate created the session and has synchronized the session to its peer. In other words for this session FGT-A, in Figure 1, is the firewall that built this session and inspection will happen on it. If we looked at the peer FortiGate, FGT-B, we would see the same session however the "synced" flag would be missing.

The new flag is important in troubleshooting since it lets us see which FortiGate is handling a particular session. When FortiGates are deployed in networks that use ECMP/multi-path routing such as in Figure 1, sessions will be built by both FortiGates and the "synced" flag is the key piece in understanding which FortiGate is handling a particular session.

FGT-A from Figure 1.

```
session info: proto=6 proto_state=05 duration=469 expire=0 timeout=3600
flags=00000000 sockflag=00000000 sockport=21 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/
state=log may_dirty ndr synced
statistic(bytes/packets/allow_err): org=544/9/1 reply=621/7/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=46->45/45->46
gwy=10.2.2.1/10.1.1.1
hook=pre dir=org act=noop 192.168.1.50:45327->172.16.1.100:21(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.1.100:21->192.168.1.50:45327(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00002deb tos=ff/ff ips_view=1 app_list=2000 app=16427
dd_type=0 dd_mode=0
per_ip_bandwidth meter: addr=192.168.1.50, bps=633
```

Session Synchronization Traffic Link

Session synchronization can take up a fair amount of bandwidth so you should use a dedicated link not data bearing interfaces. The session synchronization traffic is UDP based and there is no option for a backup link. As a result it is very important that the link between the FortiGates always be maintained. The link should be direct and not connect through other intermediate network switches.

NAT session synchronization

FGSP can synchronize NAT sessions however when taking failover into consideration extra attention to the NAT configuration is required. When using NAT in a firewall policy the default option of "Use Destination Interface Address" is not ideal. Looking at Figure 2 we can see that port1 on FGT-A and FGT-B are connected to the same layer-2 network. In a firewall policy if the default NAT option of "Use Destination Interface Address" is selected then all traffic is tied to the IP address of port1 on FGT-A. If a failure occurs on FGT-A all traffic will essentially be

black-holed since the IP address on port1 is now gone. To overcome this an Overloaded IP Pool should be used. Overload is the default type and is visible via “show full-configuration”.

```
config firewall ippool
    edit "FGSP-ippool"
        set startip 172.31.1.1
        set endip 172.31.1.254
```

Firewalling of Asymmetric Traffic

FGSP is designed to enforce firewall policy on asymmetric traffic, including cases where the TCP 3-way handshake is split between two FortiGates. Looking at Figure 3, FGT-A receives the TCP-SYN, FGT-B receives the TCP-SYN-ACK and FGT-A receives the TCP-ACK. Under normal conditions a firewall will drop this connection since the 3-way handshake was not seen by the same firewall. However two FortiGates with FGSP configured will be able to properly pass traffic since the firewall sessions are synchronized. If traffic will be highly asymmetric, as described above, the following command must be enabled on both FortiGates.

```
config system ha
    set session-pickup enable
    set session-pickup-expectation enable
```

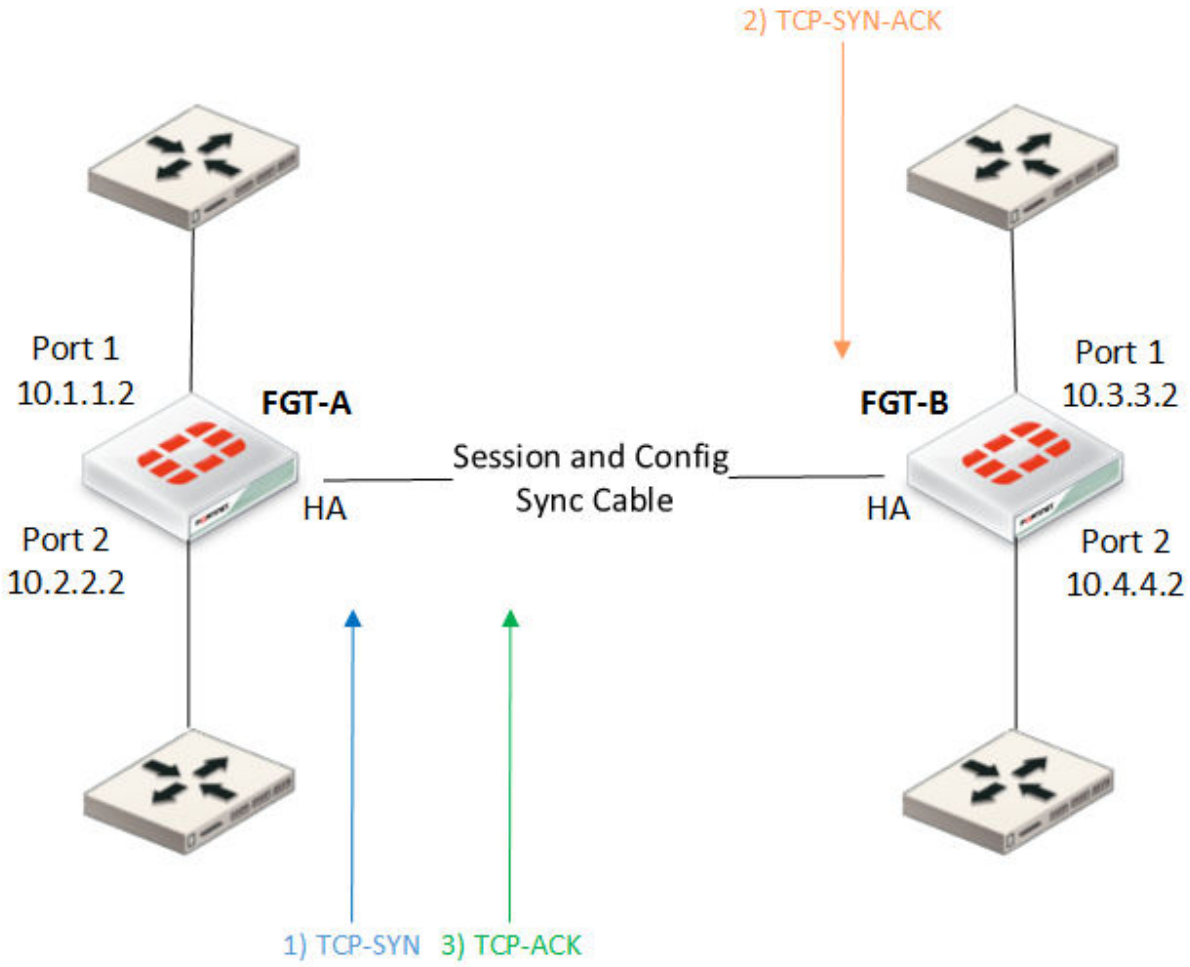
This asymmetric function can also work with UDP and ICMP traffic. The following command needs to enabled on both FortiGates.

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
```

Synchronizing asymmetric traffic can be very useful in situations where multiple Internet connections from different ISPs are spread across two FortiGates. Since it is typically not possible to guarantee Internet bound traffic leaving via an ISP will return using the exact same ISP, FGSP provides critical firewall functions in this situation.

FGSP also has applications in virtualized computing environments where virtualized hosts move between data centers. The firewall session synchronization features of FGSP allow for more flexibility than in traditional firewalling functions.

Figure 3



UTM Flow-based Inspection and Asymmetric Traffic

UTM inspection (flow or proxy based) for a session is not expected to work properly if the traffic in the session is balanced across more than one FortiGate in either direction. Flow-based UTM should be used in FGSP deployments.

For an environment where traffic is symmetric, UTM can be used with the following limitations:

1) No session synchronization for the sessions inspected using proxy-based UTM. Sessions will drop and need to be reestablished upon data path failover.

2) Sessions with flow-based UTM will failover however inspection after the failover may not work.

A single FortiGate must see both the request and reply traffic for UTM inspection to function correctly. For environments where asymmetric traffic is expected, UTM should not be used.

FGSP vs FGCP Active-Active

FGSP and FGCP are both methods for enabling high availability with FortiGate firewalls however there are differences which are important to understand. FortiGate Clustering Protocol (FGCP) is deployed using two FortiGates in either an active-passive or active-active configuration. FGCP Active-Active differs from FGSP in that FortiGates using FGCP appear as a single logical firewall to all other networking devices. Using FGCP the FortiGates share the same layer-2 and layer-3 configurations. FGCP requires that the FortiGates are layer-2 adjacent since they share a virtual MAC address in order to create a single logical firewall. These requirements when using FGCP do not work in asymmetric traffic scenarios or in situations where the FortiGates must have unique IP addresses (Figure 1) for proper function within a network. FGSP is always active-active and must be deployed using unique IP addresses on each interface.